UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

25 Swanee Lane
Thomasville, North Carolina 27360

Case No. 1:24MJ 95 -1

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

The premises located at 25 Swanee Lane, Thomasville, North Carolina 27360, more particularly described in Attachment A, attached hereto and made part hereof.

located in the Middle District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

Evidence of, instrumentalities used in committing, and fruits of the crime of 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B), all of which are more particularly described in Attachment B, attached hereto and made a part hereof.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2)(A)	Receipt of Child Pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of and Access with Intent to View Child Pornography

The application is based on these facts:

See attached affidavit incorporated by reference herein

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/S/ Cory E. Brant
Applicant's signature

Cory E. Brant, Special Agent HSI
Printed name and title

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date: 2/29/2024

Judge's signature

City and state: Winston-Salem, North Carolina

Joi Elizabeth Peake, U. S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT

FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF THE RESIDENCE, OUTBUILDINGS, AND APPURTENANCES LOCATED AT: 25 Swanee Lane Thomasville, North Carolina 27360	Case No. 1:24mj95

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Cory E. Brant, a Special Agent (SA) with Homeland Security Investigations (HSI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent of the U.S. Department of Homeland Security, Homeland Security Investigations (HSI), for approximately 22 years and am currently assigned to the Resident Agent in Charge (RAC) Greensboro, North Carolina. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center (FLETC) and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I am also a certified computer forensics and mobile device examiner and have conducted forensic analyses on over 200

electronic devices that have contained, or have been alleged to have contained, child pornography or other evidence related to the sexual exploitation of minors. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. §§ 2251(a), 18 U.S.C. §§ 2252 and 18 U.S.C. §§ 2252A, and I am authorized by law to request search and arrest warrants.

2. This affidavit is being submitted in support of an application for a search warrant for the property specifically described in Attachment A of this affidavit, including the entire property located at 25 Swanee Lane, Thomasville, North Carolina 27360 (hereinafter, the "SUBJECT PREMISES"), for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A, which items are more specifically described in Attachment B of this affidavit.

3. I am investigating the activities of Bryson J. HAWKINS, and others yet unknown, for the receipt and possession of child pornography, and I have probable cause to believe that contraband and evidence of a crime, fruits of a crime, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(2)(A) (receipt of, conspiracy to receive and distribute, and attempt to receive and distribute child pornography) and 18 U.S.C. § 2252A(a)(5)(B) (possession and access with intent to view child pornography) are located within the property described in Attachment A.

4. The statements in this affidavit are based in part on information provided to me by HSI Special Agents from Del Rio, Texas, HSI Task Force Officers from Raleigh, North Carolina, Detectives with the Davidson County Sheriff's Office, and on my own investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only

the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) are presently located within the SUBJECT PREMISES, the property described in Attachment A.

STATUTORY AUTHORITY

5. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) prohibits a person from knowingly receiving, distributing or conspiring to receive or distribute, or attempting to do so, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and

b. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

6. The following definitions apply to this affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

e. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, or circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work.

Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be "dynamic," meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer connects to the Internet.

i. "Internet Service Providers," as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

j. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

k. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

l. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives,

videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic, or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), mobile telephone devices, video gaming devices, portable music players, Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).

m. "Remote Computer Service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

n. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

o. "Storage medium" means any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

p. "Visual depiction," as define in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data store on computer disc or other electronic means which is capable

of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, THE INTERNET, AND EMAIL

7. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four (4) functions in connection with child pornography: production, communication, distribution, and storage.

b. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten (10) years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photographs taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of data or more, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard

drive in the camera. The video files can be easily transferred from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "instant messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte or larger external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files

on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache

and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

8. Based upon my training and experience, and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware

and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

9. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for contraband, evidence, fruits, or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords), so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). Further, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

10. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO POSSESS AND/OR ATTEMPT TO VIEW CHILD PORNOGRAPHY

11. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who possess and/or attempt to view child pornography:

a. Such individuals often receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals may possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children often retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the

possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[1]

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely completely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, telephone numbers, and usernames of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if

[1] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

HAWKINS or other co-conspirators use a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in the property specifically described in Attachment A of this affidavit, including the entire property located at 25 Swanee Lane, Thomasville, North Carolina 27360.

PROBABLE CAUSE

12. On September 6, 2023, HSI Del Rio, Texas, received information from the Office of the Texas Attorney General regarding the Discord account "Sketch#7254" and its involvement with child pornography. The information was received via National Center for Missing and Exploited Children (NCMEC) CyberTip 160123032, which indicated that the Discord[2] account "Sketch#7254" had uploaded files that appeared to be child pornography. Between September 11, 2023 and September 18, 2023, the Office of the Texas Attorney General provided HSI Del Rio with five additional NCMEC Cybertips that had been linked to NCMEC CyberTip 160123032 by the IP addresses 68.207.5.226 and 68.206.151.173. A summary of the five NCMEC Cybertips are listed below:

a. **NCMEC Cybertip 160123191**

Platform: Discord

Report Date: April 10, 2023 at 24:44:57 UTC
Incident Date: April 10, 2023 at 21:00:46 UTC

Suspect Info:

[2] Discord is an instant messaging and Voice Over Internet Protocol (VoIP) platform that allows users to communicate through voice calls, video calls, text messaging, files and media. Although developed for lawful purposes, the platform is also used by individuals engaged in illicit activities, to include violations of 18 U.S.C. § 2252A.

Email:	jaredtenlas@gmail.com
Screen/Username:	Sketch#7254
IP Address:	68.207.5.226
IP Address Date:	April 10, 2023 at 21:39:05 UTC
File Information:	
Filename:	xh3b5uw1vd.gif
Description:	This image file depicts a nude, prepubescent, female kneeling on a couch. A pubescent female is also visible. The pubescent female is kneeling in front of the prepubescent female while the prepubescent female has her hand touching near the pubescent female's vagina. The prepubescent female also has her face pressed against the right breast of the pubescent female.

b. **NCMEC Cybertip 160123290**

Platform:	Discord
Report Date:	April 10, 2023 at 21:48:56 UTC
Incident Date:	April 10, 2023 at 21:03:28 UTC
Suspect Info:	
Email:	jaredtenlas@gmail.com
Screen/Username:	Sketch#7254
IP Address:	68.207.5.226
IP Address Date:	April 10, 2023 at 21:03:48 UTC
File Information:	
Filename:	1654335791814.jpg
Description:	This image file depicts two nude, prepubescent, males on a bed. One of the males is straddling the other while their penises are touching.

c. **NCMEC Cybertip 160123272**

Platform: Discord

Report Date: April 10, 2023 at 21:48:48 UTC
Incident Date: April 10, 2023 at 21:03:48 UTC

Suspect Info:

Email: jaredtenlas@gmail.com
Screen/Username: Sketch#7254
IP Address: 68.207.5.226
IP Address Date: April 10, 2023 at 21:39:05 UTC

File Information:

Filename: 8k7i9jfvdgkmw.gif

Description: This image file depicts what appears to be a prepubescent child in gray colored pajamas. There is no nudity in this visual depiction provided.

d. **NCMEC Cybertip 162052442**

Platform: Twitter

Report Date: May 12, 2023 at 03:42:09 UTC
Incident Date: May 11, 2023 at 22:37:19 UTC

Suspect Info:

Email: lemonheadone@icloud.com
Screen/Username: Skezzy123423
IP Address: 68.207.5.226
IP Address Date: April 12, 2023 at 01:27:50 UTC

File Information:

Filename: dbb3Xn73.jpg

Description: This image file depicts a nude, prepubescent female wearing only white socks. The prepubescent female is sitting in the lap of a nude adult female. The prepubescent female's left hand is touching the adult female's right breast while the two kiss each other on the mouth.

e. **NCMEC Cybertip 162726458**

Platform: Snapchat

Report Date: May 25, 2023 at 01:21:20 UTC
Incident Date: May 24, 2023 at 02:58:26 UTC

Suspect Info:

Email: lemonheadone@icloud.com
Screen/Username: skeezy_007
IP Address: 68.206.151.173
IP Address Date: May 24, 2023 at 03:09:03 UTC

File Information:

Filename: skeezy_007-None-5b9478e3-1a48-53e7-b33b-ca09e37ff575-14-9d1ccf4e4d.mp4

Description: This 29-second video file depicts an adult male kneeling over a prepubescent child. For the duration of the video, the adult male is kneeling over the child violently forcing his penis into and out of the child's mouth. The child can be seen attempting to push the adult male's legs away.

Filename: skezzy_007-None-5b9478e3-1a48-53e7-b33b-ca09e37ff575-17-51f79ea545.jpg

Description: This image file depicts a nude, prepubescent male with an adult female. The adult female is lying on her back while the prepubescent male has his mouth touching the vaginal area of the adult female.

Filename: skezzy_007-None-5b9478e3-1a48-53e7-b33b-ca09e37ff575-17-a4b2dcd911.jpg

Description: This image file depicts two prepubescent females on a bed with an adult male. One of the females can be observed with her hand touching the adult male's penis. The male's penis appears to be ejaculating into the child's mouth. The second female can be seen watching the sex act being performed on the other female.

13. On October 3, 2023, HSI Special Agent Alex Stallings appeared before the Honorable Matthew Watters, United States Magistrate Judge for the Western District of Texas, and obtained a search warrant authorizing the search of the Snapchat[3] account "skeezy_007" for evidence of violations of 18 U.S.C. § 2252 and 18 U.S.C. § 2252A. On October 19, 2023, HSI Del Rio received the search warrant return from Snapchat, Inc. A review of the search warrant return revealed that the Snapchat account "skeezy_007" contained approximately seven video files and two image files depicting child pornography. Further review revealed a May 24, 2023 conversation in which the Snapchat account "skeezy_007" sent five video files and two image files depicting child pornography to the Snapchat account "bamcham2023." The following is a summary of the conversation, which occurred on May 24, 2023 between 02:51:05 UTC and 02:59:50 UTC:

Bamcham2023:	*Yo*
Skeezy_007:	*Suppp*
Bamcham2023:	*So whatcha got?*
Skeezy_007:	*Whatcha want?*
Skeezy_007:	*If weâ€™re talking about ðŸ • (copied directly from return)*
Bamcham2023:	*I want the most fucked up shit you got and as young as you got*
Skeezy_007:	*What gender*

[3] Snapchat is a multimedia instant messaging application that allows users to exchange pictures and videos that are only available for a short period of time before they become inaccessible by the recipients. Although developed for lawful purposes, the platform is also used by individuals engaged in illicit activities, to include violations of 18 U.S.C. § 2252A.

Bamcham2023: *Prefer girl but boys are cool to and also it's a plus if there crying*

Bamcham2023: *Yo you there lol*

Skeezy_007: *Was getting some shit*

Bamcham2023: *Oh ok*

Skeezy_007: *Shared the two photographs and five videos with bamcham2023.*

Bamcham2023: *0000000-0000-0000-0000-000000000000*

14. On November 27, 2023, HSI Special Agent Stallings appeared before the Honorable Matthew Watters, United States Magistrate Judge for the Western District of Texas, and obtained a search warrant authorizing the search of the Snapchat account "bamcham2023" for evidence of violations of 18 U.S.C. § 2252 and 18 U.S.C. § 2252A. On November 30, 2023, HSI Del Rio received the search warrant return from Snapchat, Inc. A review of the search warrant return revealed that it did not contain any media files for the Snapchat account "bamcham2023." Further review revealed the following:

Subscriber Identification

Username:	bamcham2023
Created On:	May 22, 2023 at 22:00:05 UTC
Creation IP Address:	65.188.235.141
Verified Email:	bamcham2229@gmail.com (verified)
Verified Date:	May 22, 2023 at 22:05:47 UTC
Display Name:	Bam Cham
Birthdate:	December 17, 1993
Last Active:	May 26, 2023 at 12:19:15 PDT

IP Address Data

IP Address:	65.188.235.141
IP Address Date:	May 22, 2023 at 22:00:05 UTC (Login)
IP Address:	2603:6081:5d00:aef3:d68:41cb:4621:a799
IP Address Date:	May 22, 2023 at 22:00:12 UTC

15. On December 4, 2023, HSI Del Rio Criminal Intelligence Analyst Marissa Guerra issued a DHS Summons to Charter Communications, Inc., requesting subscriber identification information and other user account information for IP Address 65.188.235.141 on May 22, 2023 at 22:00:05 UTC. On December 7, 2023, Charter Communications, Inc. provided the following:

Subscriber Information

Subscriber Name:	Leroy Georgia
Service Address:	25 Swanee Lane Thomasville, North Carolina 27360
Username:	jamalgeorgia31@gmail.com
Phone Number:	336-491-6382

16. On December 22, 2023, HSI Del Rio sent a collateral request to HSI Greensboro, North Carolina, requesting the investigation of the Snapchat account "bamcham2023" for violations of 18 U.S.C. § 2252 and 18 U.S.C. § 2252A. On or about this same date, HSI Del Rio submitted an investigative packet to HSI Greensboro. A review of the packet revealed that it contained the seven child pornography files that had been sent by Snapchat account "skeezy_007" to Snapchat account "bamcham2023" on May 24, 2023. I have personally viewed each of these files and have confirmed that they depict child pornography, as defined in 18 U.S.C. § 2256(8). Following are three descriptions of the video files that were viewed:

a. **File Name:** *skeezy_007-None-5b9478e3-1a48-53e7-b33b-ca09e37ff575~16-b7cff808f5.mp4*

Description: This 12-second video depicts a child, approximately three to nine months old, lying on its back while an adult male places his erect penis in its mouth. The child can be observed sucking on the penis as if she were breastfeeding.

b. **File Name:** *skeezy_007-None-5b9478e3-1a48-53e7-b33b-ca09e37ff575~16-397881b695.mp4*

Description: This 31-second video depicts a child, approximately 9-15 months of age, completely naked and being held by what appears to be an adult female. The child is facing the adult female and is being held in a manner in which the child is bent at the waist, head down, with their exposed anus facing outward. An adult male can be seen attempting to insert his erect penis into the child's anus. As the video continues, the adult female can be seen spreading the child's buttocks and anus open, allowing the adult male to insert his penis in the child's anus. The child can be heard screaming and crying.

c. **File Name:** *skeezy_007-None-5b9478e3-1a48-53e7-b33b-ca09e37ff575~14-9d1ccf4e4d.mp4*

Description: This 29-second video depicts a child, approximately 3-9 months of age, naked from the waist up and lying on its back. An adult male can be observed straddling the child. As the adult male straddles the child, they can be observed using one hand to place their erect penis in the child's mouth and the other hand to hold the back of the child's head and force it up and down. As the child's head goes up and down, the erect penis can be seen going in and out of the child's mouth. The child can be seen hitting and pushing the adult in an attempt to stop the abuse.

On January 10, 2024, HSI Greensboro Criminal Intelligence Analyst Tracy Randecker issued a DHS Summons to Google LLC, requesting subscriber identification information and other user account information for the email address "bamcham2229@gmail.com," the verified email address associated with the Snapchat account "bamcham2023." On or about January 25, 2024, Google LLC provided the following:

Subscriber Information

Name:	Bam Cham
Given Name:	Bam
Family Name:	Cham
Email Address:	bamcham2229@gmail.com
Alternate Email:	None
Created On:	May 21, 2023 at 02:40:40 UTC
IP Address:	2603:6081:5d00:aef3:a903:7abd:247a:6f2d

IP Address Data

IP Address:	2603:6081:5d00:aef3:428:e215:50ab:4e0
IP Address Date:	May 28, 2023 at 10:11:47 UTC
IP Address:	2603:6081:5d00:aef3:6d69:8f08:f3cd:107a
IP Address Date:	May 27, 2023 at 09:03:51 UTC May 26, 2023 at 08:45:31 UTC May 25, 2023 at 08:08:12 UTC May 24, 2023 at 07:55:56 UTC
IP Address:	2603:6081:5d00:aef3:a903:7abd:247a:6f2d
IP Address Date:	May 21, 2023 at 02:44:53 UTC May 21, 2023 at 02:42:21 UTC May 21, 2023 at 02:42:18 UTC May 21, 2023 at 02:42:05 UTC May 21, 2023 at 02:42:03 UTC May 21, 2023 at 02:40:41 UTC

17. On January 26, 2024, HSI Greensboro Criminal Intelligence Analyst Randecker issued a DHS Summons to Charter Communications, Inc., requesting subscriber identification information and other user account information for the below listed IP Addresses, which were associated with login/logout records for the email address "bamcham2229@gmail.com:"

a. 2603:6081:5d00:aef3:428:e215:50ab:4e0
May 28, 2023 at 10:11:47 UTC

b. and 2603:6081:5d00:aef3:6d69:8f08:f3cd:107a

May 24, 2023 at 07:55:56 UTC.

On or about February 1, 2024, Charter Communications, Inc. provided the following for both IP Addresses:

Subscriber Information

Subscriber Name:	Leroy Georgia
Service Address:	25 Swanee Lane Thomasville, North Carolina 27360
Username:	jamalgeorgia31@gmail.com
Phone Number:	336-491-6382

18. On or about February 15, 2024, I received information from the Davidson County Sheriff's Office indicating that a search of the Thomasville City Schools database revealed that Bryson J. HAWKINS (DOB: 09/22/2005) was currently residing at the 25 Swanee Lane, Thomasville, North Carolina 27360 (the SUBJECT PREMISES).

19. On or about this same date, I conducted law enforcement databases queries and discovered that on August 26, 2022, the Raleigh, North Carolina, Police Department (RPD) had arrested HAWKINS and charged him as a juvenile with 16-counts of Second-Degree Sexual Exploitation of a Minor, a violation of North Carolina General Statute § 14-190.17 (distribution and receipt of a visual representation of a minor engaged in sexual activity).

20. On February 23, 2024, I received copies of investigative reports from RPD Detective/HSI Task Force Officer Lindsay Faust documenting the investigation of HAWKINS and his August 26, 2022 arrest. According to the reports, on July 7, 2022, RPD executed a state search warrant at 10311-101 Arrow Creek Drive, Raleigh, North Carolina 27617 for crimes related to the Sexual Exploitation of a Minor. During the execution of the warrant, RPD Detective encountered

and interviewed HAWKINS. During the interview, HAWKINS admitted to possessing and distributing child pornography on a regular basis and having a collection of over 1,000 videos depicting child pornography. Based upon the severity of child pornography located and the extreme volume of child pornography being possessed and distributed, the Assistant District Attorney recommended that HAWKINS be charged on juvenile petitions.

MANNER OF SEARCHING COMPUTER SYSTEMS

21. As described in Attachment B, this application seeks permission to search for records that might be found at the SUBJECT PREMISES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

22. *Probable cause.* I submit that if a computer or storage medium is found at the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

23. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about when the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether

the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data also typically contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping"

program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

24. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make

an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the SUBJECT PREMISES. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

25. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

26. Because several people may share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

PROCEDURE FOR UNLOCKING ENCRYPTED DEVICES

27. The search warrant requests authorization to use the biometric unlock features of a device (including phones and computers), as described in Attachment B, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices (including phones and computers). To use this function, a user generally displays a

physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

28. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress Bryson J. HAWKINS' thumb and/or fingers on the device(s); and (2) hold the device(s) in front of Bryson J. HAWKINS' face with his eyes open to activate the facial-, iris- and/or retina-recognition feature.

CONCLUSION

29. Based on the aforementioned information, I respectfully submit that there is probable cause to believe that contraband, evidence, fruits, and instrumentalities of offenses in violation of 18 U.S.C. § 2252A, as more fully described in Attachment B of this Affidavit, may be located at the residence described in Attachment A.

30. I, therefore, respectfully request that the attached warrant be issued authorizing the search of the SUBJECT PREMISES and the seizure of the items listed in Attachment B to include a full forensic examination of any computers, electronics, and related devices listed here.

/S/ Cory E. Brant
Cory E. Brant
Special Agent
Homeland Security Investigations

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this 29 day of February 2024, at 3:21 a.m./p.m.

Joi Elizabeth Peake
United States Magistrate Judge
Middle District of North Carolina

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The entire property located at 25 Swanee Lane, Thomasville, North Carolina 27360, including the residence, any outbuildings, and/or other structures within the property's curtilage, and any appurtenances thereto (all which constitute the SUBJECT PREMISES). Local law enforcement and/or task force officers will be utilized in order to ensure execution of the search warrant at the correct physical location.

The SUBJECT PREMISES, 25 Swanee Lane, Thomasville, North Carolina 27360 is a single-story residence constructed of red brick with greenish blue shutters and front door. The front door, which faces west, is protected by a black storm door. The driveway to the residence is located on the right side of the residence and ends in a single vehicle car port. A photograph of the residence is reproduced below:

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252A(a)(2)(A) and 2252A(a)(5)(B):

1. Computers or storage media used as a means to commit the violations described above.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER and/or how and when the COMPUTER was used at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. evidence indicating the computer user's knowledge and/or intent as to the crime(s) under investigation, such as research into child exploitation statutes;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

i. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

j. records of or information about Internet Protocol addresses used by the COMPUTER;

k. records of or information about the COMPUTER's Internet activity, specifically: firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses revealing an interest in child exploitation content; and

l. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography, as defined in 18 U.S.C. § 2256(8), and child erotica (including on the computers or storage media as defined herein).

5. Records, information, and items relating to violations of the statutes described above in the form of:

a. Records and information referencing child pornography, as defined in 18 U.S.C. 2256(8);

b. Records and information referencing child erotica;

c. Records, information, and items referencing or revealing the occupancy or ownership of 25 Swanee Lane, Thomasville, North Carolina 27360, including utility and telephone bills, mail envelopes, or addressed correspondence;

d. Records, information, and items referencing or revealing the ownership or use of computer equipment found in the above residence, specifically: sales receipts, bills for Internet access, and handwritten notes;

e. Records and information referencing or revealing the identity or location of the persons suspected of violating the statutes described above;

f. Records and information referencing or revealing the sexual exploitation of children;

g. Records and information revealing sexual interest in minors;

h. Records and information referencing or revealing trafficking, advertising, or possession of child pornography, to include the identity of the individuals involved and location of occurrence;

i. Records and information referencing or revealing communication or interaction of an illicit sexual nature with minors, to include the identity of the individuals involved and location of occurrence;

j. Records and information constituting or revealing membership or participation in groups or services that provide or make accessible child pornography; and

k. Records and information revealing the use and identification of remote computing services such as email accounts or cloud storage; and

g. Records and information pertaining to the Snapchat account "Bamcham2023."

6. During the course of the search, photographs of the searched premises may be taken to record the condition thereof and/or the location of items therein.

As used above, the terms "records" and "information" includes all forms of creation or storage, specifically: any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies); and any cloud storage (which the aforementioned electronic devices are connected to).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions,

including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro-SD cards, macro-SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

During the execution of the search of the SUBJECT PREMISES described in Attachment A, law enforcement personnel are also specifically authorized to compel Bryson J. HAWKINS, if present at the time of the execution of the warrant, to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

a. any of the devices found at the SUBJECT PREMISES, and

b. where the devices are limited to which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the devices' security features in order to search the contents as authorized by this warrant, but only if Bryson J. HAWKINS is present at the time of the execution and the process is carried out with dispatch in the immediate vicinity of the SUBJECT PREMISES.

This warrant does not authorize law enforcement personnel to compel any other individuals found at the SUBJECT PREMISES to provide biometric features, as described in the preceding

paragraph, to access or otherwise unlock any device. Further, this warrant does not authorize law enforcement personnel to request that any individuals present at the SUBJECT PREMISES state or otherwise provide the password or any other means that may be used to unlock or access the devices, including by identifying the specific biometric characteristics (including unique finger(s) or other physical features) that may be used to unlock or access the devices.